BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75755 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IT00/00216

(22) International Filing Date: 25 May 2000 (25.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO99A000480 8 June 1999 (08.06.1999) IT

(71) Applicant *(for all designated States except US)*: EUTRON INFOSECURITY S.R.L. [IT/IT]; Via Gandhi, 12, I-24048 Cumasco di Treviolo (IT).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LEIDI, Michele [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Cumasco di Treviolo (IT). CASSIA, Lucio [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Cumasco di Treviolo (IT).

(74) Agent: GARAVELLI, Paolo; A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).

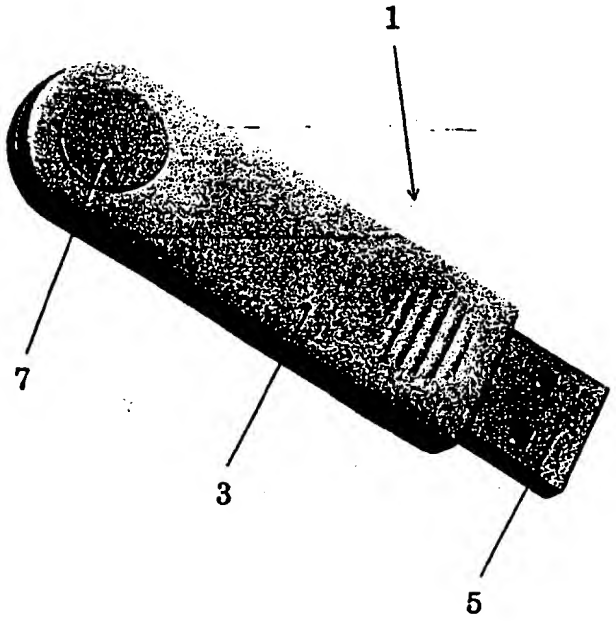
(81) Designated States *(national)*: AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: IDENTIFICATION DEVICE FOR AUTHENTICATING A USER



(57) Abstract: A device (1) is described to authenticate a user in an Internet environment, comprising: a support structure (3); a terminal (5) for the connection to a processor port; a microprocessor circuitry to perform safety functions and cryptography algorithms; and activation means (7) to allow enabling an authentication code. A system and a process are further described to input a PIN inside the device (1) and a system and a process to authenticate a user based on such device (1).

WO 00/75755 A1

IDENTIFICATION DEVICE FOR AUTHENTICATING A USER

The present invention refers to a user authentication system within an Internet architecture based on an hardware device connected to the Universal Serial Bus (USB) port of a client processor through a cryptographic procedure of the "Challenge Response" type. Moreover, the invention refers to a hardware and software system to input a Personal Identification Number (PIN) inside the above-said identification device based on USB port in order to prevent the interception thereof.

With the always wider spreading of the Internet network and other networks of this type, a particular and major importance has been given to problems about the controlled distribution of information on the network, in order to guarantee that these information cannot be attacked and guarantee their privacy as well, in addition to

providing access to particular transactions or information only to authorised users. Several arrangements have so far been proposed, starting from the so-called protecting "hardware keys" to be connected to processors, up to more or less complex cryptographic systems with different types of software keys. The proposed solutions either are very costly to be implemented in terms of several types of resources, or do not guarantee a complete safety of the information to be protected.

Object of the present invention is solving the above prior-art problems, by providing an hardware and software system that is of a reduced cost, easily implemented and absolutely efficient in terms of protection. In particular, the hardware device of the invention is of a simple configuration, has the sizes of a key and, once being inserted into the USB port of a computer, allows univocally recognising and authenticating the user of a network-based application and to start therewith protected and encrypted transactions on the Internet network itself. Authentication uniqueness and transaction safety are based on the features of the device, that is equipped with a microprocessor implemented for

safety functions, and on private-key time-varying cryptographic algorithms.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a user authentication device and process as claimed in Claims 1 and 6, respectively, and by a system and process that use the above device as claimed in Claims 15 and 17, respectively. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of the device according to the present invention;
- Figure 2 is a block diagram of the architecture of the code-inputting system of the device of the invention;
- Figure 3 is a block diagram of the process realised by the architecture in Fig. 2;
- Figure 4 is a block diagram detailing a step of the process in Fig. 3;

- Figure 5 is a block diagram detailing a step of the process in Fig. 3;
- Figure 6 is a block diagram of the operating process of the device in Fig. 1;
- Figure 7 is a block diagram detailing a step of the process in Fig. 6;
- Figure 8 is a block diagram detailing a step of the process in Fig. 6;
- Figure 9 is a block diagram summarising the steps of the processes in Fig.s 7 and 8; and
- Figure 10 is a block diagram detailing a step of the process in Fig. 6.

With reference to Fig. 1, the device 1 for authenticating a user in an Internet architecture environment substantially comprises an elongated support structure 3, preferably made of plastic material and adapted to be grasped by a user and inserted into a port of a client processor (not shown), for example the Universal Serial Bus (USB) port of a personal computer. For such purpose, the device 1 is equipped with a terminal 5 for the connection to the port and with a microprocessor circuitry contained inside the support structure 3; the circuitry is adapted to perform safety

functions and to operate on cryptographic algorithms. Finally, the device 1 of the invention comprises activation means 7 (commonly realised in the shape of a push-button) supported by the structure 3 and adapted to control the microprocessor circuitry to allow enabling therein an authentication code, as will be described hereinbelow.

In the current and preferred embodiment, the device 1 operates on cryptographic algorithms that are of the private-key time-varying type. Due to the standard interface and "plug&play" USB and to a set of interfacing libraries of the ActiveX and Plug-In type on server and client sides, the device 1 is efficient in terms not only of safety, but also of simplicity and transparency. Its features make it an efficient tool to store keywords, electronic certificates, digital signatures, electronic purse functions or to store and protect therein other interesting information related to user or used services.

With the device 1 of the invention, those who need protecting and checking the access to pages, services, data bases or more generally to areas of Internet sites, will simply have to supply

authorised users of their one Internet service with a suitably initialised device 1. The users will then have to simply insert the device 1 into the USB port of the computer without performing any installation operation. The server application will take care of setting a safe communication with the device 1 in order to authenticate the user. User recognition in fact occurs depending on reserved information inside the device linked with a user keyword. Once having recognised the client and having checked affected user authorisations, the device 1 takes care of sending customised and reserved information to the user, encrypting the contents with an algorithm of the 256-bit Blowfish type, for example, with a time-varying key linked to the secret value contained into the device 1. Information can be indifferently, but not in a limiting way, HTML pages, data bases information with "web" interface, forms, download areas, and the like. The information transaction of the network is performed encrypted both from server to client, and vice versa.

In order to be able to use the above-described device 1, it is necessary to equip it with a univocal Personal Identification Number (PIN) per

user. For such purpose, a system has been implemented whose architecture is shown in Fig. 2, such system being adapted to perform a process as detailed in Figures 3 to 5.

With reference first of all to Fig. 2, the system architecture that allows using the device 1 substantially comprises a processor equipped with a graphic window 10 that displays a digit from 0 to 9. Such window cooperates with a user library 12 (arrow A in Fig. 2), that is a proprietary library that deals with managing the device 1 and, through an identification process 14 contained therein, with checking the enabling of the device 1 itself.

The user library 12 is connected (arrow B in Fig. 2) with a device driver 16, that is also a proprietary library that deals with managing the device 1 at USB level. The device driver 16 is connected (arrow C in Fig. 2) with the device 1 that receives commands (arrow D in Fig. 2) from the push-button 7. According to the flow defined by arrows A to D, in the user library 12 an internal tick pulse is generated so that, upon every tick, a digit is sent both to the window 10 for being displayed, and to the device 1 through the device driver 16; the device driver 16 queries the device

1 whether there are other digits and, if the response is affirmative, goes on with the processing, while otherwise it warns the user library 12 to stop the process. Upon every pressure of the push-button 7, the device 1 stores the currently supplied digit that is also displayed by the window 10.

The general operation of the above-described system is shown as a block diagram in Fig.s 3 to 5. Such process guarantees the maximum safety when inputting the PIN to use the device 1. The process first of all comprises, upon request of the PIN code, the activation (301) of the graphic window 10 to display a current digit from 0 to 9.

Then the PIN code is sent (303) for every digit, through a process inserted into the libraries, both to the displaying window 10 and to the device 1.

Upon pressing the push-button 7, therefore, every digit is stored (305) as belonging to the PIN code; then, the process that sends the digit both to the graphic window 10 and to the device 1, queries (307) every time the device 1 to check whether there are other digits: if the response is affirmative, the process goes on by timely sending

(309) the other digits; otherwise, it stops (311) and the final PIN key is stored to validate the device 1.

Upon a more detailed examination, the operation of the PIN code storing step (305) can be divided into two major steps, where the first one deals with managing the display and dispatch of the digits to the device 1, while the second one deals with managing the push-button 7 of the device 1 itself.

In particular, as shown in detail in Fig. 4, the displaying and dispatching step of the digits to the device 1 starts in 401 and comprises the following sub-steps:

- creating (403) the window 10 to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response, removing (407) the displaying window 10; or
- in case of a negative response, sending (409) the digit to the graphic window 10 and to the device 1; and
- requesting (411) to the device 1 whether the

digits limit for the PIN code has been reached, returning to the querying step (405): if the response is affirmative, the process finally ends in 413.

With reference to Fig. 5, instead, the flow diagram of the management step for the push-button 7 of the device 1 is shown in detail, this step being able to be divided into the following sub-steps, starting from the initial one in 501:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response, ending (509) the process; or
- in case of a negative response, checking (505) whether the push-button 7 has been pressed;
- in case of a negative response, the procedure remains waiting for a following pressure of the push-button 7; or
- in case of an affirmative response, storing (507) the last received digit and returning to the querying step (503) are performed.

After having defined the device 1 of the invention in this way and the system and process to

store and validate the personal code inside the device, it is possible to practice the real and proper process of the invention to manage the accesses to reserved pages and services being present on the Internet network.

As already stated, the system that allows such process is composed, preferably but not in a limiting way, of a central server processor (not shown) that stores and manages the authorised users, connected to a set of local client processors (not shown) equipped with the device 1 of the invention. The detailed procedure is commonly realised through programs being present on both server and client processors, and is shown in Fig.s 7 to 10 of the description.

In particular, with reference to Fig. 6, the process for authenticating a user in an Internet architecture environment comprises the following macro-steps:

- associating (601) a user with an identification device 1;
- identifying (603) the user through the device 1; and
- encrypting (605) information sent/received by/from the user.

In particular, as shown in Fig. 7, the associating step (601) of a user to the device 1 comprises the following sub-steps:

- describing (701) the user;
- generating (703) a TokenId based on describing data of the user;
- performing (705) a first irreversible safe scrambling step (preferably of the MD5 type) of the TokenId after a communication (709) with the server processor managing the keywords;
- creating (706) a first Personal Identification Number (PIN) from the first scrambling (705);
- performing (707) a second irreversible safe scrambling step (preferably of the MD5 + 3DES type) of the TokenId after a communication (709) with the server processor for the keywords;
- creating (708) a second Personal Identification Number (PIN2) from the second scrambling (705), where the second Personal Identification Number (PIN2) is different from the first Personal Identification Number

(PIN);

- associating the user with an identification string composed of the TokenId, the first Personal Identification Number (PIN) and the second Personal Identification Number (PIN2); and
- storing such complete identification string into the device 1 and the TokenId alone into a data base on the server processor.

With reference now to Fig. 8 in particular and to Fig. 9 as assembly view of the two steps shown in Fig.s 7 and 8, the user identifying step (603) through the device 1 is shown in detail; it comprises the following sub-steps:

- in case of an access by the user to web pages of the network in which an access control must be performed, the server processor sends (801) to the client processor a string of the "Server Challenge" type, that is always different; the string is associated with the first Personal Identification Number (from 706) and is processed by the client to be able to provide a response for the server. For this purpose, the process proceeds with the steps of:

- performing (803) an hashing step (preferably of the MD5 type) on the "Server Challenge" string and the first Personal Identification Number, thereby producing (805) a text string;
- using (807) the second Personal Identification Number (PIN2) (from 708) as encrypting key of a cryptography (809) (preferably of the 3DES type) on the text string;
- generating (811, 813) a string comprising the TokenId and a Response Client and sending such string to the server processor;
- comparing (step 901 in Fig. 9) on the server the received string with the Response Client being generated on the server side by re-processing the first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to such comparing step (901), pointing out (step 903 in Fig. 9) the existence of a correct identification code; or
- in case of a negative response to such comparing step (901), pointing out (step 905

in Fig. 9) the existence of an incorrect or counterfeited identification code.

Finally, with reference to Fig. 10, the information encrypting step (605) comprises the following sub-steps, performed by the server processor:

- generating (1000) an encryption key from the previous encrypting step (809) by using as input the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page from the network;
- encrypting (1001) (preferably using the Blowfish encryption) the received page through the generated encryption key; and
- sending (1005) the encrypted page to the client processor, which, once having received the encrypted pages, is able to decrypt them and reproduce them in a clear way, because it knows both the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2).

Some embodiments of the invention have been described, but obviously they are subjected to further modifications and variations within the

same inventive idea. For example, several construction variations of the device 1 will be possible, both from the point of view of the connections to external processor ports, and from the point of view of the internal circuitry to realise the described functionalities. Moreover, the various processes of the invention could be applied to various types of authentication devices, and the systems to realise the described processes could be implemented according to different connection configurations to various types of networks.

CLAIMS

1. Device (1) for authenticating a user in an Internet architecture environment, characterised in that the device comprises:

- a support structure (3);
- a terminal (5) for the connection to a port of a processor;
- a microprocessor circuitry contained inside said support structure (3), said circuitry being adapted to perform safety functions and operating on cryptographic algorithms; and
- activation means (7) supported by said structure (3) and adapted to control said microprocessor circuitry to allow enabling therein an authentication code.

2. Device (1) according to Claim 1, characterised in that said terminal (5) is adapted to be connected to a port of the Universal Serial Bus (USB) type of a personal computer.

3. Device (1) according to Claim 1, characterised in that said activation means (7) are composed of a push-button.

4. Device (1) according to Claim 1, characterised in that said cryptographic algorithms performed by said microprocessor circuitry are of the private-key time-varying type.

5. Device (1) according to Claim 3, characterised in that said cryptographic algorithms are of the "Challenge Response" type.

6. Process for authenticating a user in an Internet architecture environment, characterised in that the process comprises the following steps:

- associating (601) a user with an identification device (1);
- identifying (603) said user through said device (1); and
- encrypting (605) information sent/received by/from said user.

7. Process according to Claim 6, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

8. Process according to Claim 6, characterised in that said associating step (601) comprises the following sub-steps:

- describing (701) said user;
- generating (703) a TokenId based on describing data of said user;
- performing (705) a first irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor;
- creating (706) a first Personal Identification Number (PIN) from said first scrambling (705);
- performing (707) a second irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor, said second scrambling (707) being different from said first scrambling (705);
- creating (708) a second Personal Identification Number (PIN2) from said second scrambling (705), said second Personal Identification Number (PIN2) being different from said first Personal Identification Number (PIN);
- associating said user with an identification string composed of said TokenId, said first Personal Identification Number (PIN) and said

second Personal Identification Number (PIN2); and

- storing said complete identification string into said device (1) and said TokenId into a data base on said server processor.

9. Process according to Claim 8, characterised in that said first scrambling (705) is of the MD5 type and said second scrambling (707) is of the MD5 + 3DES type.

10. Process according to any one of Claims 6 to 9, characterised in that said identifying step (603) comprises the following sub-steps:

- in case of an access by said user to pages of said network in which an access control must be performed, sending (801) by the server processor a string of the "Server Challenge" type, said string being associated with said first Personal Identification Number;
- performing (803) an hashing step on said "Server Challenge" string and said first Personal Identification Number, thereby producing (805) a text string;
- using (807) said second Personal Identification Number (PIN2) as encrypting

key of a cryptography (809) on said text string;

- generating (811, 813) a string comprising said TokenId and a Response Client and sending said string to said server processor;
- comparing (901) said received Response Client string with the Response Client being generated on the server side by re-processing said first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to said comparing step (901), pointing out (903) the existence of a correct identification code; or
- in case of a negative response to said comparing step (901), pointing out (905) the existence of an incorrect or counterfeited identification code.

11. Process according to Claim 10, characterised in that said hashing is of the MD5 type and said cryptography (809) is of the 3DES type.

12. Process according to any one of Claims 6 to 11, characterised in that said encrypting step (605) comprises the following sub-steps, performed by said server processor:

- generating (1000) an encryption key from said encrypting step (809) by using as input said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page of said network;
- encrypting (1001) said received page through said generated encryption key; and
- sending (1005) said encrypted page to said client processor, said client processor being able to perform the decrypting of said encrypted page depending on said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2) being known thereto.

13. Process according to Claim 12, characterised in that said encrypting (1001) is of the Blowfish type.

14. System for authenticating a user in an Internet architecture environment, characterised in that the system comprises:

- at least one central management server processor connected in a network;
- at least one local client processor connected

in the network;

- at least one authentication device (1) according to any one of Claims 1 to 5 connected to said at least one local client processor; and
- a control program adapted to perform the process according to any one of Claims 6 to 13.

15. System for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the system comprises, connected to said device (1), a processor containing:

- at least one user library (12) for managing said device (1), said user library (12) being equipped with an identification process (14) adapted to control the enabling of said device (1);
- at least one device driver (16) connected to said user library (12), said device driver (16) being a library that manages said device (1) at connection port level; and

- at least one window (10) connected to said user library (12) to display said PIN code digit by digit.

16. System according to Claim 15, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

17. Process for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the process comprises the following steps:

- upon request of said PIN code, activating (301) a graphic window (10) to display an current digit from 0 to 9;
- sending (303) every digit of said PIN code both to the displaying window (10) and to the device (1);
- in case of actuation of activation means (7) of said device (1), storing (305) every digit as belonging to said PIN code;
- querying (307) said device (1) to check whether other digits exist;
- in case of an affirmative response to said

querying step (307), timely sending (309) the other digits; or

- in case of a negative response to said querying step (307), stopping (311) the process and storing the final PIN key to validate said device (1).

18. Process according to Claim 17, characterised in that said PIN code storing step (309) comprises the following steps:

- displaying and dispatching the digits to said device (1); and
- managing the activation means (7) of said device (1).

19. Process according to Claim 18, characterised in that said displaying and dispatching step of the digits to said device (1) comprises the following sub-steps:

- creating (403) a window (10) to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (405), removing (407) said displaying window (10); or

- in case of a negative response to said querying step (405), sending (409) the digit to said graphic window (10) and to said device (1); and
- requesting (411) to said device (1) whether the digits limit for the PIN code has been reached, returning to said querying step (405).

20. Process according to Claim 18, characterised in that said managing step of the activation means (7) of said device (1) comprises the following sub-steps:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (503), ending (509) said process; or
- in case of a negative response to said querying step (503), checking (505) whether said activation means (7) are actuated;
- in case of a negative response to said checking step (505), suspending the procedure that remains in stand-by; or
- in case of an affirmative response to said

checking step (505), storing (507) the last received digit and returning to said querying step (503).

21. Process according to Claim 17, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

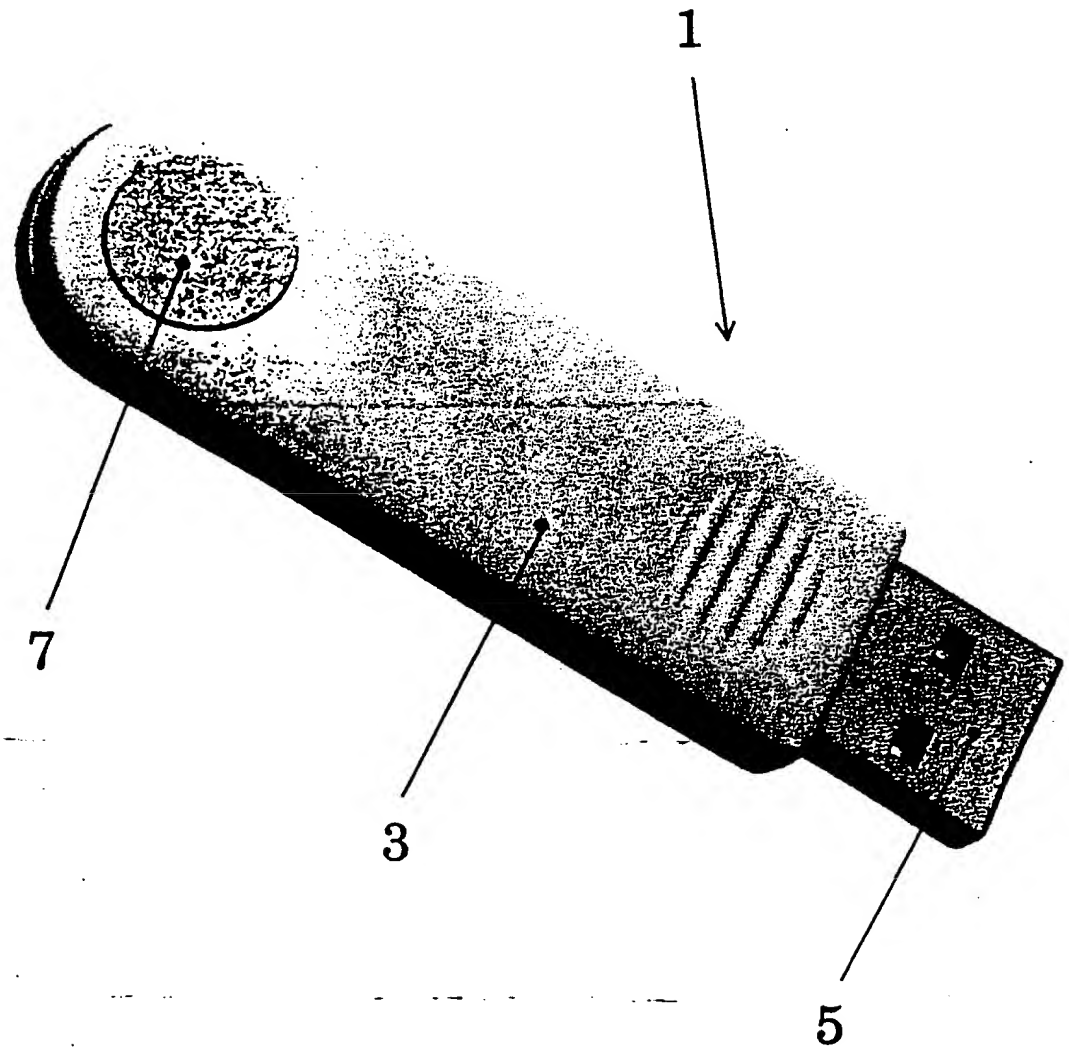


Fig. 1

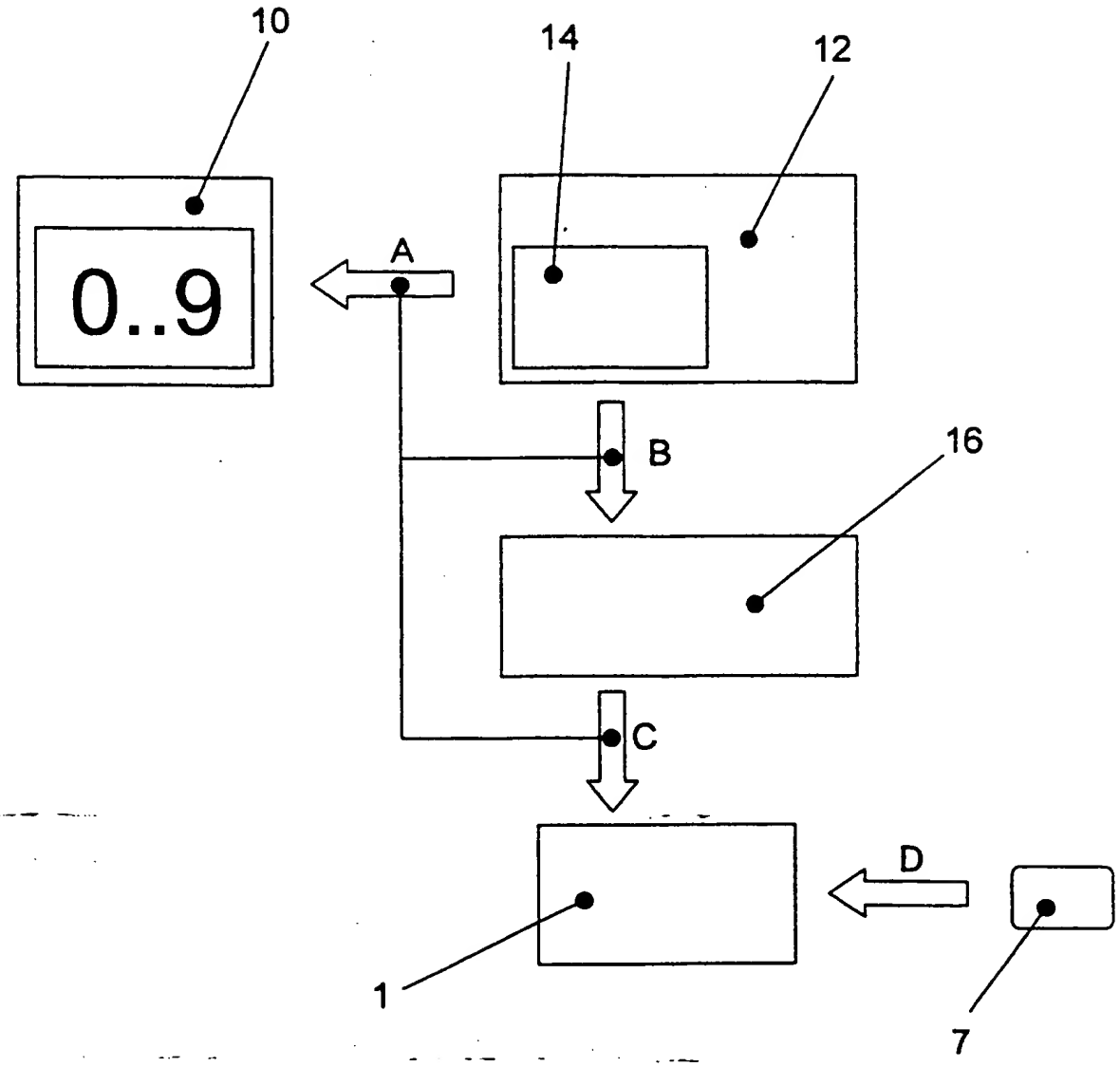


FIG. 2

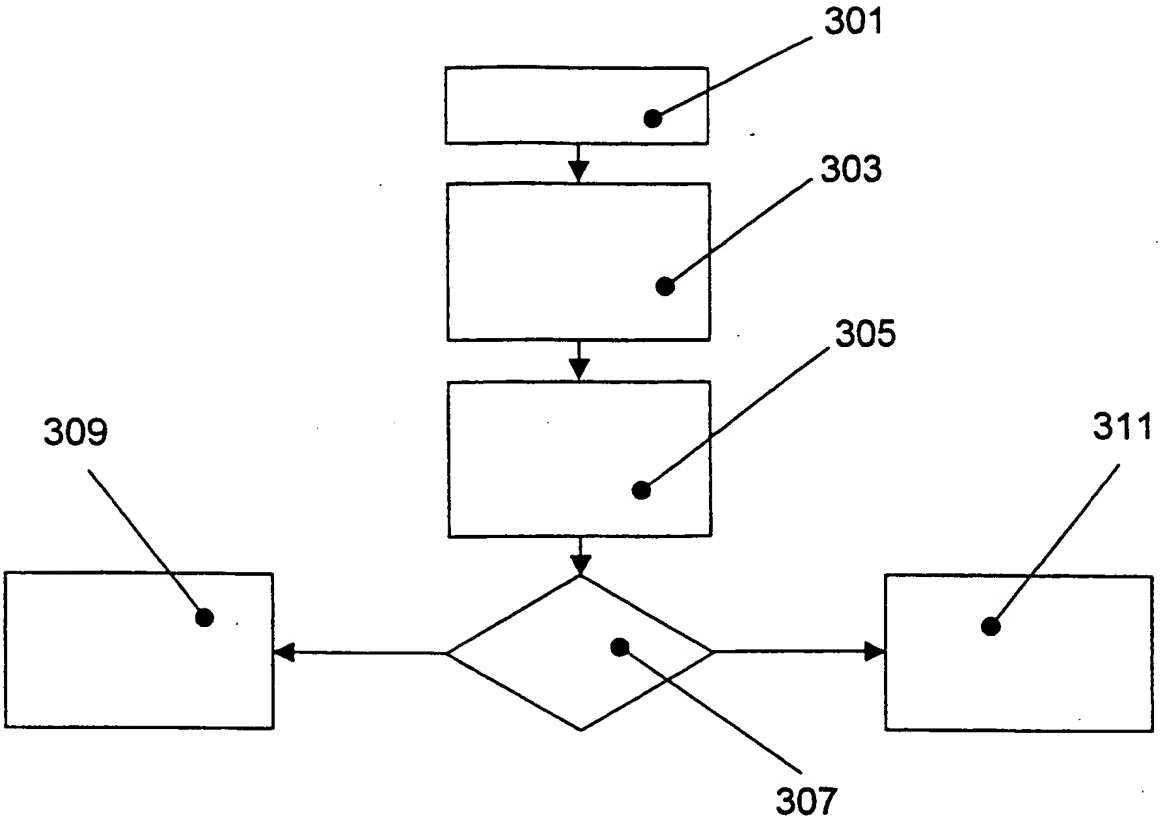


FIG. 3

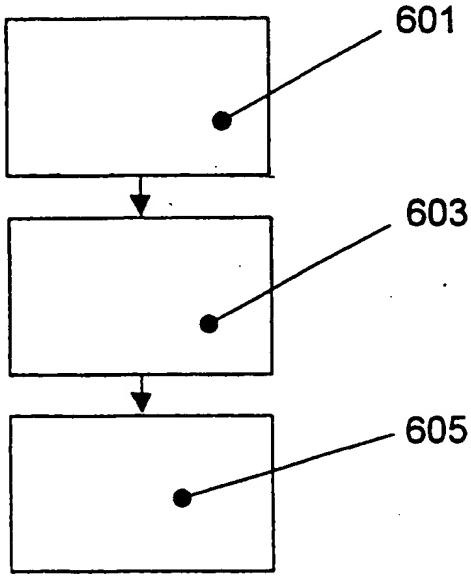


FIG. 6

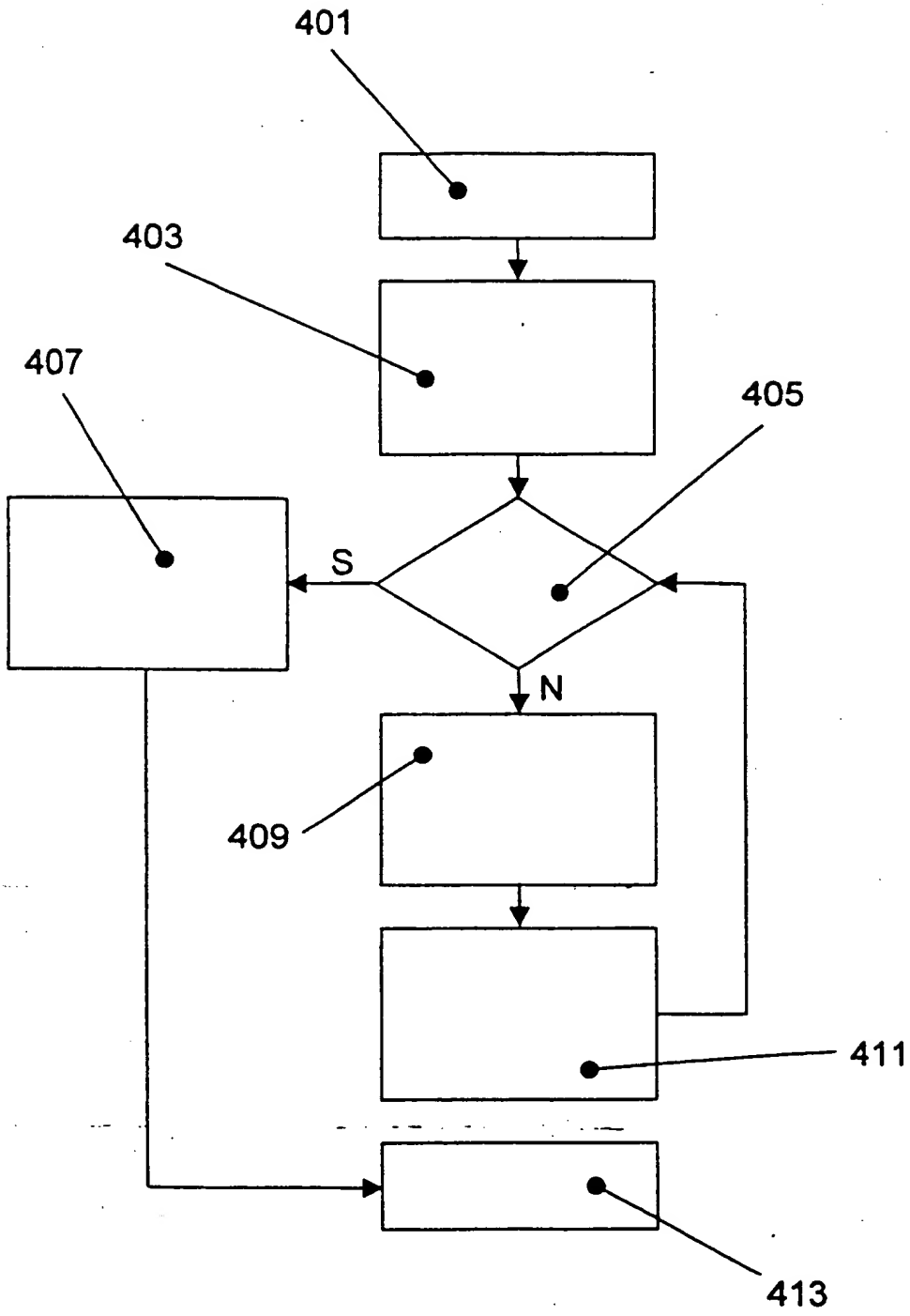


FIG. 4

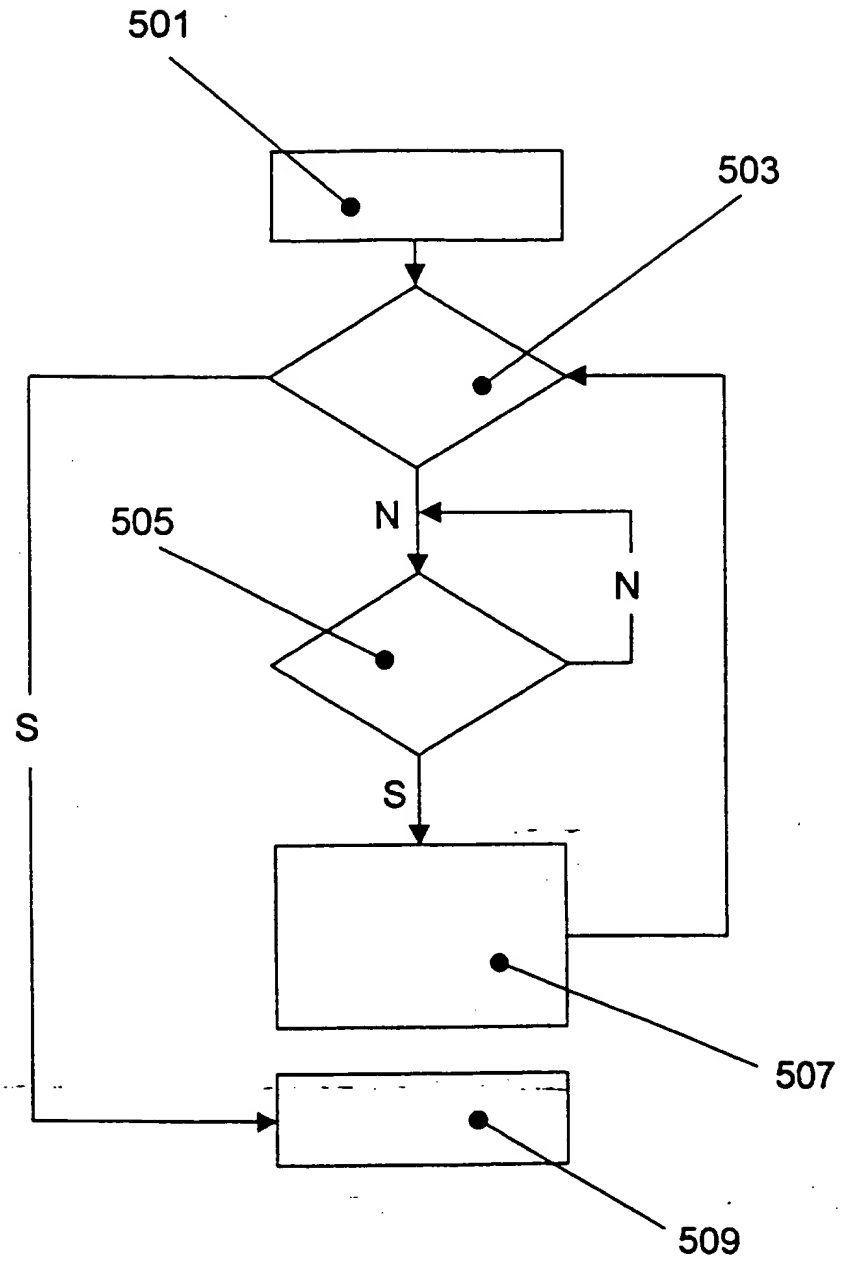


FIG. 5

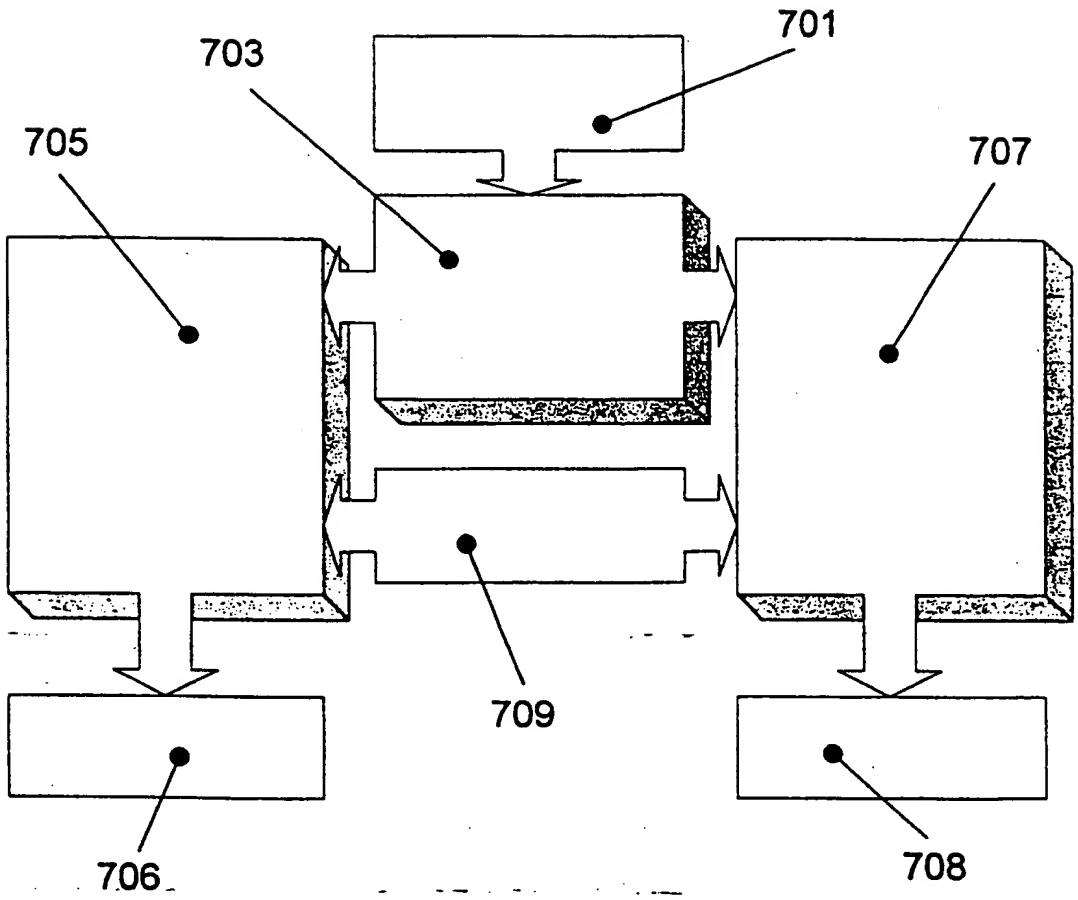


FIG. 7

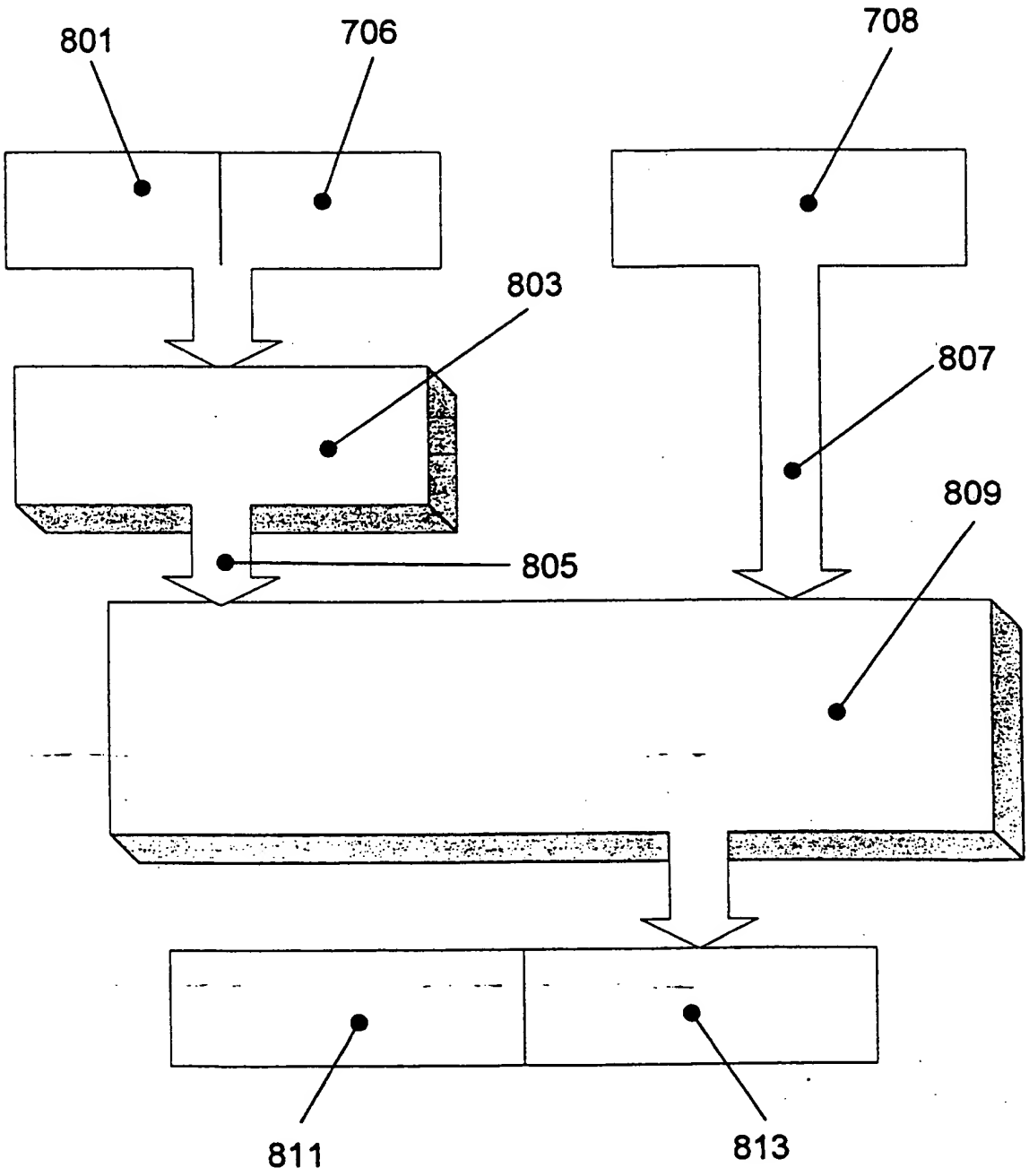


FIG. 8

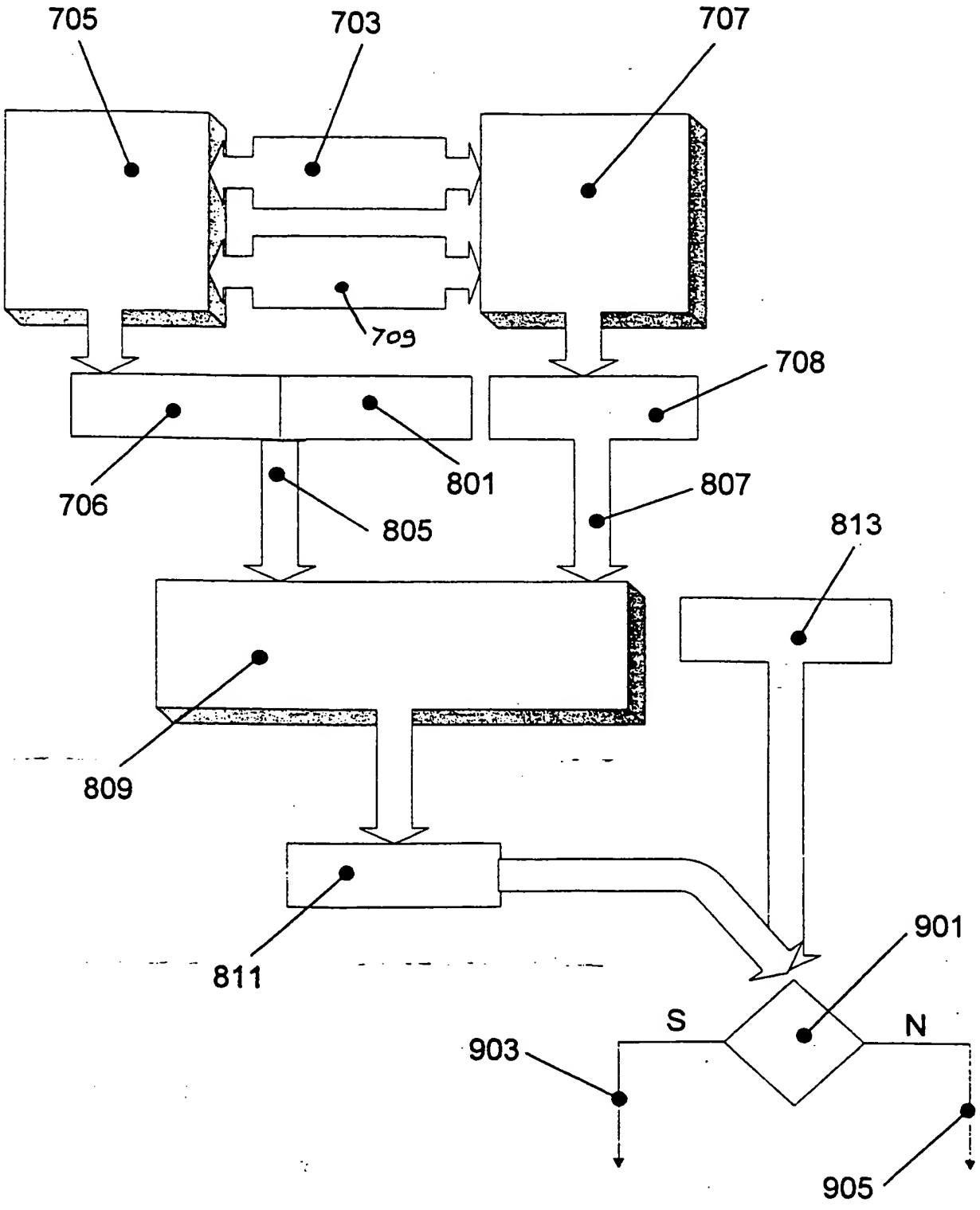


FIG. 9

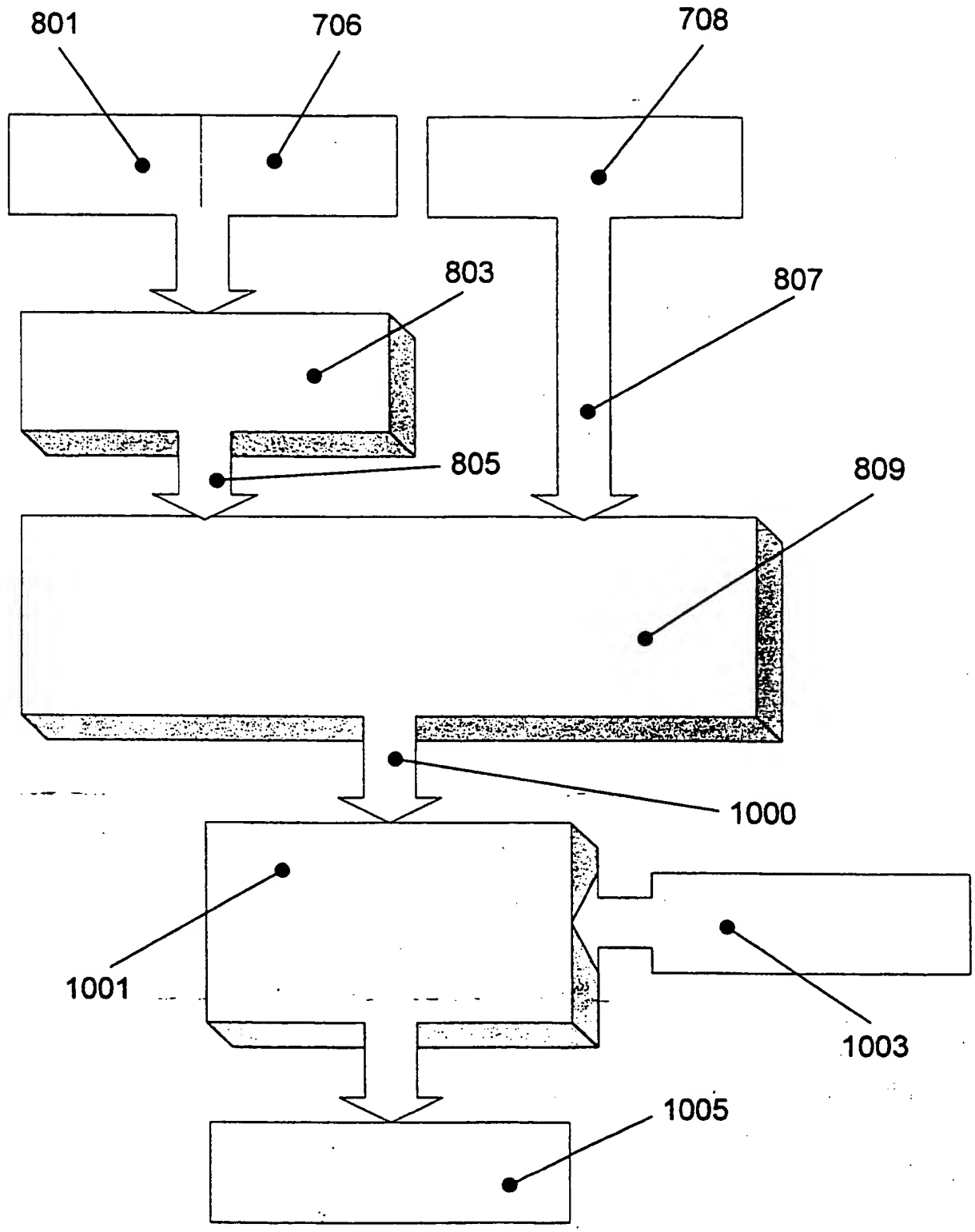


FIG. 10

INTERN ONAL SEARCH REPORT

tional Application No
PCT/IT 00/00216

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 778 071 A (CAPUTO ET AL) 7 July 1998 (1998-07-07) column 7, line 21 - line 36 column 10, line 51 -column 12, line 22 column 13, line 4 -column 18, line 9; figures 1D,2,4,5-8	1,3-7,14 8-13, 15-21
A	L. PREUSS: "Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 17 November 1998 (1998-11-17), XP002139273 the whole document	1,2,4-7, 14,15,17

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2000	02/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IT 00/00216

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 (1991-10-22) column 4, line 6 -column 5, line 24	15,17
E	WO 00 42491 A (RAINBOW TECHNOLOGIES INC) 20 July 2000 (2000-07-20) page 16, line 16 - line 20; claims 1-3,5,6; figures 7,8	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IT 00/00216

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5060263 A	22-10-1991	NONE	
WO 0042491 A	20-07-2000	NONE	